Circuit Authentication and Identification using Innovative Built-in Self-Test (BIST) Techniques

Esko Mikkola
Doohwang Chang
Richard Welker
Andrew Levy
Alphacore, Inc.
Tempe, AZ 85281
esko.mikkola@alphacoreinc.com

Sule Ozev
Jennifer Kitchen
Andrew Hoyt
Arizona State University
Tempe, AZ 85287
sule.ozev@asu.edu

***Abstract*— This paper describes circuit-level built-in self-test (BIST) techniques for (a) monitoring the performance of RF devices, including LNAs, mixers, and oscillators, (b) assigning unique identification numbers to chips using on-chip monitor information, and (c) algorithms to authenticate/identify chips through the supply chain and estimate remaining lifetime in the field. These techniques increase the confidence for system performance not only at the time of system integration, but also through the entire operation. The information from the monitors will be used to predict the remaining lifetime of the device. A mechanism for multi-variate unique identifier that can authenticate chips at the time of system integration is described that is based on combining the statistical variation in all parameters. Combination of this unique ID with in-field aging data enables tracking and identification of chips in the supply chain even after they have been used in the field. The paper shows results of analyses of device-specific and process-specific measurements that ensure that the goals of monitoring performance, unique identification, and device authentication are met when using the proposed methodologies and tools.**

Keywords—circuit authentication, circuit identification, multi-variate analysis, cybersecurity, low-noise amplifier, built-in self-test (BIST), built-in current sensor (BISC), built-in amplitude analysis (BIAS), counterfeiting, tampering

I. INTRODUCTION

The integrated circuit (IC) design industry has adopted a globalized design and manufacturing flow where multiple design teams contribute to the design of one IC, which gets fabricated in an off-site facility, and possibly tested in another. While such a distributed flow helps meet the stringent time-to-market deadlines and offer a financially viable model, it is also vulnerable to various forms of security threats in the supply chain that involves designers, fabs, test facilities, and distributors until the end-product reaches the customers. These threats include insertion of malicious circuitry in the IC, also known as hardware Trojans, intellectual property (IP) piracy, IC overproduction by the foundry to make additional profit via sales in aftermarket, and counterfeit ICs. Among these security threats, the most prominent one has been the counterfeit ICs. Aged, rejected, or cloned parts, also known as counterfeit chips, find their way into the supply chain and pose a big threat to profitability, security and reliability of electronic products [1-5].

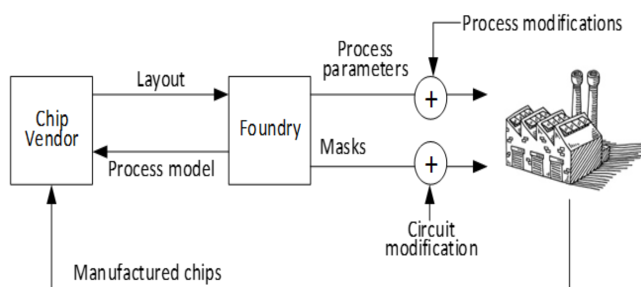


Figure 1. Cybersecurity Threat Model

Distribution Statement A. Approved for public release: distribution is unlimited.

II. THREAT MODEL

Figure 1 illustrates our threat model. The IC vendor receives the process model from the foundry and produces the layout of the circuit based on this process model. The threats originate at the foundry due to malicious attackers (third-party consultants, rogue employees) or due to non-malicious quality control issues. Process variables, such as doping concentration and annealing temperature, can be altered, resulting in small global shifts in circuit component parameters. The circuit itself can be altered during mask generation by inserting unwanted circuit components (e.g., dipole antennas, capacitive loading), or by changing the attributes of connections (e.g., wire thickness). If the modification is nefarious, the goal of the attacker is to weaken the manufactured circuit such that it fails shortly after deployment or becomes easier to tamper with externally. The attacker can make process changes intermittently throughout the production cycle to avoid detection. Hence, all chips manufactured by an untrusted foundry are suspect until verified otherwise.

III. PROPOSED AUTHENTICATION METHOD

Our model for authentication is “trust-but-verify”. During the design process, the IC vendor develops enhanced test modes and statistical authentication models based on the process design kit (PDK) provided by the foundry, which may not be fully trusted. Upon receiving manufactured devices, the IC vendor randomly samples devices from each lot and authenticates each sample with respect to these test modes and

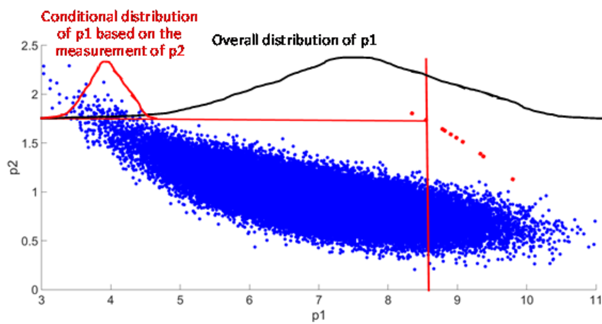


Figure 2: Outlier analysis to detect process and circuit changes that alter relations between performance parameters.

authentication models that are not disclosed to the foundry. If a device fails this authentication step, further analysis is conducted to diagnose the potential causes. One cause may be a false alarm due to the statistical nature of the authentication models. However, this failure may be due to an alteration to the circuit or process that is not authorized by the IC vendor. This diagnosis step can involve invasive techniques, such as accelerated aging, over-stress testing, delayering, and X-ray inspection, and may require more time and resources as it is encountered infrequently.

A. Multi-Variate Analysis

Malicious or unintentional changes to process and circuit variables, such as dopant concentration, channel length, metal thickness, annealing time, and temperature can be used to lower resilience to in-field degradation mechanisms, such as hot carrier injection, oxide breakdown, negative bias temperature, and electromigration. These changes in the process result in minor variations in the circuit response that can be hidden within overall process variations, thus making the changes extremely difficult to detect [6-11]. However, in the field, these weaker circuits may fail quickly, due to the exponential relationship between process parameters and degradation. In [11], the authors have developed a model linking modified process parameters to in-field lifetime and have shown that lifetime is reduced drastically. Such modifications are referred to as Process Reliability Trojans [6-11]. One possible way of addressing the detection of such reliability Trojans is to include additional transistors and extensively test their characteristics for manufactured ICs. However, this would be costly in terms of area/pin overhead.

Fortunately, for RF circuits, changes in almost every process variable will result in some change in performance parameters. If the process shift and/or circuit modification alters the relationship between measurable performances, it can be detected via multivariate analysis, even if the deviation in each performance parameter is within process limits. As an example, Figure illustrates the scatter plot between two performance parameters (p1 and p2) that are correlated through the process. The blue dots are samples that stem from the same functional relation between these two performance parameters, and the red dots show samples that stem from a slightly altered functional relation. In a traditional test flow, p1 and p2 are measured and compared with their limits independently. In such a flow, *none*

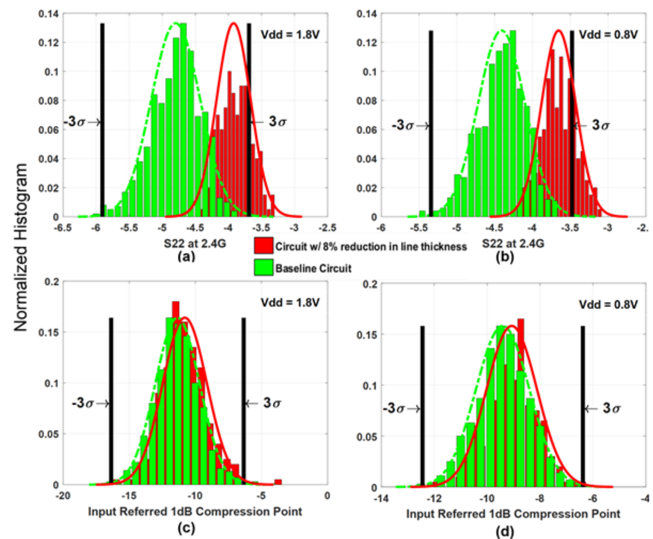


Figure 3: Two LNA performances for nominal process (green histogram) and process modified by decreasing the line thickness by 8% (red histogram) for two supply levels.

of the red dots will be flagged as suspicious as both p1 and p2 are well within their 3σ limits. For instance, the overall distribution of p1 is shown as the black probability density function. While checking against limits is ineffective, we can observe, via visual inspection, that these samples are outliers. Of course, for dimensions greater than three, visual inspection is not possible. We would like to develop an automated method to do the same using more dimensions than three. If the joint distribution of p1 and p2 are collapsed based on the measurement result of p2 for one of the red samples, the resulting conditional probability is shown as the red distribution curve. The actual location of that sample in the p1 dimension is well outside the expected conditional probability distribution. Hence, we can identify this red sample as not conforming to the expected distribution. Here, the challenge is to select a subset of parameters that will provide good fidelity for detecting process and circuit alterations. For the same example in Figure , if p2 is chosen as a target for the conditional probability, the rightmost red dot cannot be identified as an outlier.

B. Enhanced Test Modes for Increased Process Sensitivity

While designers strive for process robustness at nominal operating conditions, such as supply voltage, noise, temperature, same robustness is generally difficult to maintain over a large variation in operating conditions. By modifying these operating conditions during testing, we can increase sensitivity to process parameters. This sensitivity increase is only temporary and does not result in degradation of circuit performance. Using modified operating conditions for detecting process reliability Trojans has been deemed ineffective for digital circuits [6-11]. However, prior work on this subject has focused only on the analysis of delay-based failures, which is a discrete function of path delays and only one-dimensional. For RF circuits with many measurable performance parameters, modified operating conditions enable better detection.

As an example, Figure shows two performance parameters, output reflection coefficient (S22) and 1dB gain compression input point (P1dB), of an LNA circuit under the nominal supply voltage of 1.8V and reduced supply voltage of 0.8V. Green samples are generated via Monte-Carlo sampling using the provided PDK for TowerJazz 180nm technology. Red samples are results obtained when the line thickness of inductors is decreased by 8%, which is a small change. Both performance parameters are affected by the process change, as expected. However, a majority of the samples from the modified process fall squarely within the 3σ limits of the nominal process at both supply voltages. This process modification is not detectable using the two aforementioned measurements at either supply voltage. As a matter of fact, it is not detectable by comparing all performance parameters at any supply voltage. However, by merging the information from all measurements using a multivariate statistical model, such minute changes become detectable.

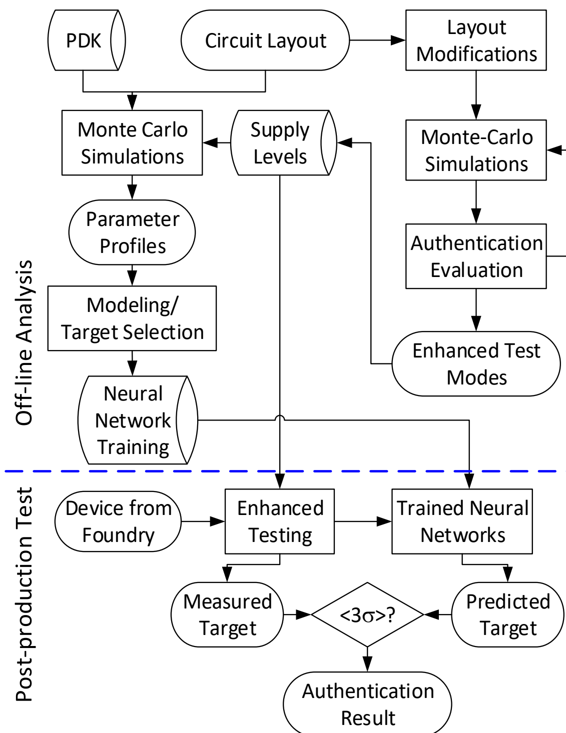


Figure 4: Proposed authentication flow

C. Authentication Flow

The proposed authentication framework consists of an off-line stage, where the circuit is analyzed under enhanced test modes and the statistical model is generated, and an on-line stage where the devices that return from the foundry are subjected to enhanced testing. The majority of the computational burden, such as training a neural network (NN), takes place during the off-line stage. The online stage post-processing poses negligible computational overhead.

Figure 4 shows the flow of the proposed authentication method. Once the circuit layout is finalized, Monte-Carlo simulations are conducted to form the statistical model and select target/input combinations. Authentication efficacy based on a number of circuit/layout modifications is also evaluated to remove test modes that do not contribute to the coverage. At the end of the off-line stage, a number of NNs are trained for prediction. Once devices are returned from the foundry, samples are taken from each lot for authentication testing (with enhanced test modes). The trained NNs are used to predict the targets and compared with the measurements to determine whether the part is authentic.

In essence, the NN collapses the joint probability distribution around each measurement, except for the target parameter and predicts what the target parameter should be using the learned correlations from simulations. If the target parameter's prediction and actual measurement differ substantially, then the circuit under test is not from the learned distribution. Hence, we can conclude that there has been a modification to either the process or the circuit.

D. Built-in Self Test Design

In order to evaluate our methodology, we use a Low Noise Amplifier (LNA) circuit. The first LNA was designed at the layout level using TowerJazz 180nm SiGe BiCMOS technology. A similar LNA is currently being developed in the TSMC 180nm CMOS process and was taped out in November 2018. The initial LNA exhibited performance issues which have been corrected for the TSMC version. In addition, the TSMC version incorporates Built-in Self-Test (BIST), Built-in Current Sensor (BISC), and Built-in Amplitude Sensor (BIAS) circuitry (Figure).

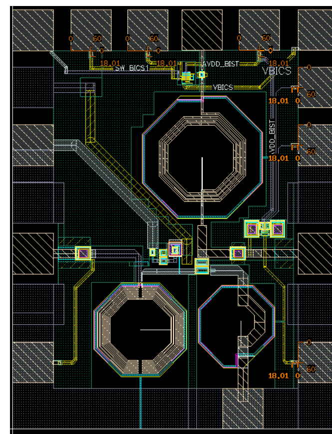


Figure 5. Layout of LNA + authenticity circuits

Three versions of the LNA (one with intentional line width variation and one with load variance) will also be taped out to demonstrate the capability of the on-chip authenticity circuitry to detect "tainted" chips. The additional circuits do not affect the area consumed by the LNA and have been designed to minimize the impact on the performance of the LNA.

The BIST modules (BICS and BIAS) integrated with the 2.4GHz LNA is designed in a TSMC 0.18-μm CMOS process. The BIST system consists of measurement circuits of DC current and amplitude, and switches and traces to direct the signal flow. The top-level of BIST system with an LNA as the DUT is shown in Figure 6. Especially, there are three configurations for BICS and BIAS:

1. The normal operation mode of DUT, where the DUT input and output are connected to functional input and output nodes and the BIST circuit is turned off to save power.

   → SW_bypass and SW1 are ON and SW2/3 are OFF

2. The calibration mode of BICS loop, where the BICS signal source (I_{CAL}) is connected to the measurement system for calibration of BICS, and DUT is turned off.

   → SW_bypass and SW2 are OFF and SW1 is ON

3. The testing mode of BIST/DUT loop, where the nominal signal source drives the input of the DUT, and the bias current and output amplitude of the DUT drives the measurement system (BIST) to generate low frequency output from BIST.

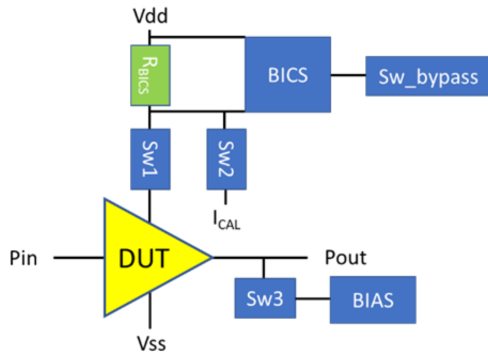


Figure 6. Top-level system for BIST with 2.4Ghz LNA

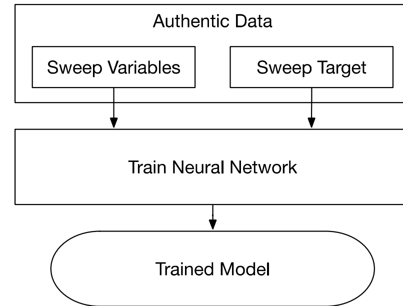
E. Authentication algorithm

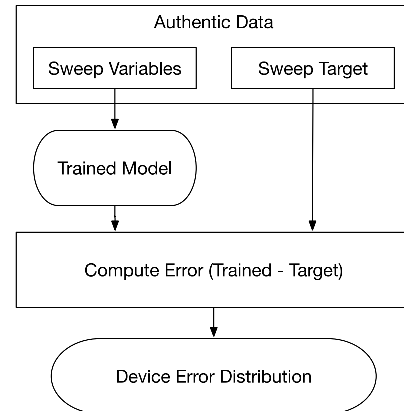
To design our circuits with BIST, we must decide which parameters are essential to measure. Some of the parameters may not be feasible to measure via on-chip circuitry. However, we may be able to measure them via a load-board. An example is Noise Figure, which generally requires a well characterized noise diode to make the measurements. The noise diode can be placed on the board, which would complicate the authentication process. To avoid unnecessary complication, we need to evaluate the cost/benefit of each measurement.

We have completed the algorithm used for classification and are preparing a publication of our findings. The algorithm differs slightly from previously reported methods, but it can be generalized in three steps (Figure 7):

1. Simulation data are collected and trained into a neural network. Common parameters such as Noise Figure, S11, S22, etc. are referred to herein as "Sweep Variables." We also define a "Sweep Target," which shares a common basis with all Sweep Variables. The Sweep Target is the set of supply levels for which all the Sweep Variables were collected. For example, parameters like S11 and S22 were simulated over five different mission and non-mission mode supply levels. These data are used to train a neural network called the "Trained Model."

2. The Authentic device data are applied to the Trained Model, and a statistical distribution is created. This distribution represents the "best-case" error in the





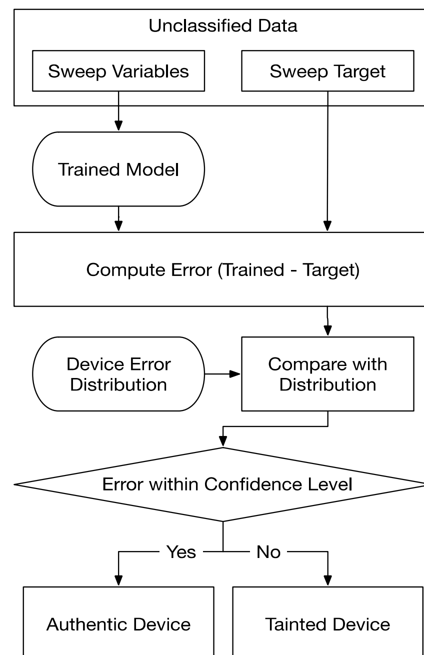


Figure 7: Authentication algorithm with reduced testing

model for authentic devices. In other words, the Trained Model will have some built-in error after evaluation, so we create a statistical distribution that can be used to set our error acceptance threshold. Practically speaking, we may choose a threshold of 99.5% of all devices in the distribution as our limit for authentic devices.

3. The final step is to classify devices using the model and distributions from steps 1 and 2. Figure 7 shows the algorithm used to preform classification. The main difference in this step is that we have determined our baseline for authentic measurements and we are now comparing that baseline to measurements that have not yet been classified.

IV. Experimental Results

As our model requires a Neural Network to process the inputs, some random variation is injected into the system as a result of training the network. To prove that this variation is manageable, we tested N different models with the same data and compared the authentication accuracy generated by the algorithm to the ideal authentication accuracy. The non-authentic data used for this comparison was comprised of modifications to capacitance and linewidth in simulation. Table 1 shows the amount of error (i.e., total misclassification) for 200 trained models and 190 sample devices.

The mean error and standard deviation for each test condition are less than 1%, which is close to the detection limit and a major improvement over the previous method. In particular, the accuracy for linewidth modification goes from a maximum of 80% to a maximum of over 94% in the worst case, and over 99% on average. With this optimized method, we have a well-defined metric for authentication accuracy that can be used to directly and accurately compare various combinations of input parameters. Table 2 shows authentication accuracy versus excluded measurement parameters.

As expected, decreasing the total number of measurements in the model shows a corresponding decrease in authentication accuracy in Linewidth simulations. Capacitance data, which have showed little deviation in the past, maintain this trend. By determining the minimum number of parameters required for authentication, we reduce the amount of on-chip testing time by selecting only the needed measurements.

Table 2: Validation of authentication accuracy with Neural Network variation

Classification Error (N=100 Models/Test Param.)				
Test Param.	Min.	Mean	Max.	S.D.
Capacitance	< 0.01%	0.01%	0.16%	0.03%
Linewidth	0.01%	0.46%	5.5%	0.84%

Table 1: Effects of excluding measurement data on accuracy. Top: Linewidth-change Comparison. Bottom: Capacitance-change comparison

Classification Accuracy (Linewidth, N=20 Networks)				
Excluded Meas.	Min.	Mean	Max.	S.D.
Noise Figure	97.6%	99.4%	99.9%	0.4%
S11	96.8%	99.4%	99.9%	0.4%
S22	96.4%	98.9%	99.9%	0.8%
NF, S11, S22	92.2%	97.5%	99.9%	1.1%
Classification Accuracy (Capacitance, N=20 Networks)				
Excluded Meas.	Min.	Mean	Max.	S.D.
Noise Figure	99.9%	99.9%	100%	0%
S11	99.9%	99.9%	100%	0%
S22	99.9%	99.9%	100%	0%
NF, S11, S22	99.9%	99.9%	100%	0 %

With the final version of the classification algorithm, we have managed to reduce classification error to negligible levels compared with our previous submissions.

The method presented here has extremely high detection capability, identifying linewidth changes of 15% and load changes of 30 fF with more than 99% accuracy. All accuracies listed in previous reports for advanced test modes have been surpassed for this section, and we are currently working to more clearly define our absolute detection limit in the context of our completed algorithms.

V. Conclusions

In this paper, we present an RF circuit authentication method based on multiple parametric measurements with enhanced test modes and machine-learning based statistical analysis. Enhanced test modes that are used in this work non-functional supply levels. In addition to the functional supply level, four additional supply levels are used to increase the behavioral diversity of devices based on process variations. Moreover, to reduce the overhead of built-in test, an algorithm has been developed to reduce the number of test measurements as well as optimize the type of test measurements by excluding hard-to-measure parameters, such as reflection coefficients and noise figure. An LNA is designed together with a BIST circuit capable of measuring supply current, DC offset, as well as the gain of the circuit. Post-layout simulations are performed on the baseline LNA as well as several copies of this device with layout modifications in the inductors and output capacitances.

Experimental results have shown that with the help of the enhanced test modes, authentication accuracy can be increased even with reduced testing of the LNA.

VI. Acknowledgements

The work described in this paper was funded by U.S. Air Force contract FA8650-16-M-1788 and now funded by FA8650-18-C-1139 under SBIR program AF161-140.

VII. References

[1] J. Roy, F. Koushanfar, and I. Markov, “EPIC: Ending Piracy of Integrated Circuits,” IEEE/ACM DATE, pp. 1069–1074, 2008.

[2] R. Chakraborty and S. Bhunia, “HARPOON: An Obfuscation-Based SoC Design Methodology for Hardware Protection,” IEEE TCAD, vol. 28, no. 10, pp. 1493–1502, 2009.

[3] M. Pecht and S. Tiku, “Bogus: electronic manufacturing and consumers confront a rising tide of counterfeit electronics,” IEEE Spectrum, vol. 43, no. 5, pp. 37–46, 2006.

[4] R. Karri, J. Rajendran, K. Rosenfeld and M. Tehranipoor, “Trustworthy Hardware: Identifying and Classifying Hardware Trojans,” IEEE Computer, vol. 43, no. 10, pp. 39-46, Dec. 2010.

[5] M. Tehranipoor and F. Koushanfar, “A survey of hardware Trojan taxonomy and detection,” IEEE Des. Test Comput., pp. 10–25, 2010.

[6] S. Ghandali, G. T. Becker, D. Holcomb, and C. Paar, “A Design Methodology for Stealthy Parametric Trojans and Its Application to Bug Attacks” CHES 2016, vol. 8086, pp. 197–214. Springer, Heidelberg.

[7] R. Kumar, P. Jovanovic, W. P. Burleson, and I. Polian, “Parametric trojans for fault-injection attacks on cryptographic hardware” IACR Cryptology ePrint Archive, p.783. 2014.

[8] Shiyanovskii, Y. *et.al.*, W. Process reliability based trojans through NBTI and HCI effects. In IEEE Adaptive Hardware and Systems Conference (pp. 215-222), 2010.

[9] Becker, G. T., *et.al.*, Stealthy dopant-level hardware trojans. In International Workshop on Cryptographic Hardware and Embedded Systems (pp. 197-214), 2013.

[10] S. Bhasin and F. Regazzoni, “A survey on hardware trojan detection techniques,” in IEEE International Symposium on Circuits and Systems pp. 2021–2024, 2015.

[11] Balasch, B. Gierlichs, and I. Verbauwhede, “Electromagnetic circuit fingerprints for hardware trojan detection,” in IEEE International Symposium on Electromagnetic Compatibility, pp. 246–251, 2015.